



FortiClient EMS for Chromebooks - Release Notes

Version 1.2.2

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



November 07, 2017

FortiClient EMS for Chromebooks 1.2.2 Release Notes

04-122-456948-20171107

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported platforms	5
System requirements	5
Domain requirements	6
Supported Web Browsers	6
Licensing and installation	6
What's New	7
Redesigned navigation menu	7
New Dashboard	7
Upgrade	8
Upgrading from previous FortiClient EMS for Chromebooks versions	8
Upgrading from previous FortiClient EMS versions	8
Downgrading to previous versions	8
Resolved Issues	9
Known Issues	10

Change Log

Date	Change Description
2017-11-07	Initial release.

Introduction

FortiClient Enterprise Management Server for Chromebooks (FortiClient EMS for Chromebooks) is used to centrally manage FortiClient for Chromebooks. You can deploy FortiClient to Chromebook devices and use FortiClient EMS for Chromebooks to import users from Google domains and centrally provision FortiClient configuration.

FortiClient offers a web filtering feature based on FortiGuard categories. EMS administrators can allow, warn, or block web categories and define exceptions as needed. Administrators can use FortiClient EMS for Chromebooks to enforce safe search on the Chrome browser.

Like standard FortiClient EMS, EMS for Chromebooks runs on Microsoft Windows Server 2008 R2 and above. It officially supports all Chromebook devices.

This document provides the following information for FortiClient EMS for Chromebooks 1.2.2 build 0443:

- [Introduction on page 5](#)
 - [Supported platforms on page 5](#)
 - [System requirements on page 5](#)
 - [Domain requirements on page 6](#)
 - [Supported Web Browsers on page 6](#)
 - [Licensing and installation on page 6](#)
- [What's New on page 7](#)
- [Upgrade on page 8](#)
- [Resolved Issues on page 9](#)
- [Known Issues on page 10](#)

For information about FortiClient EMS, see the *FortiClient EMS for Chromebooks 1.2.2 Administration Guide*.

Supported platforms

The FortiClient EMS for Chromebooks server can be installed on the following platforms:

- Microsoft Windows Server 2008 R2 or newer

System requirements

The minimum system requirements are as follows:

- 2.0 GHz 64-bit processor with dual core (or two virtual CPUs)
- 8 GB RAM (8 GB RAM or higher is recommended)
- 40 GB free hard disk
- Gigabit (10/100/1000baseT) Ethernet adapter
- Internet access

Internet access is required during installation. This becomes optional once installation is complete.



You should only install EMS and the operating system's default services on the server. You should not install additional services on the same server as EMS.

Domain requirements

The following FortiClient platforms are supported for Google domain users managed by FortiClient EMS for Chromebooks:

- Google Chromebook

Supported Web Browsers

The latest version of the following web browsers can be used to connect remotely to FortiClient EMS for Chromebooks 1.2.2 GUI:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Internet Explorer is no longer recommended. Remote access may need to be enabled from the FortiClient EMS for Chromebooks GUI.

Licensing and installation

For information on licensing and installing FortiClient EMS for Chromebooks, see the *FortiClient EMS for Chromebooks Administration Guide*.

What's New

The core features of the FortiClient EMS for Chromebooks 1.2.2 include the following:

Redesigned navigation menu

The left navigation menu has been redesigned to provide easier access to the content pane on the right. The top menu has also been merged into the left navigation menu.

New Dashboard

The new Dashboard includes new chart designs and easier access to information and alerts. Administrators can customize the dashboard by moving widgets around.

Upgrade

Upgrading from previous FortiClient EMS for Chromebooks versions

FortiClient EMS for Chromebooks 1.2.2 supports upgrading from the following FortiClient EMS for Chromebooks versions:

- 1.0.3 and later
- 1.2.0 and later

It is recommended to perform the upgrade on a staging server before upgrading the production server. See the *FortiClient EMS for Chromebooks Administration Guide*.

Upgrading from previous FortiClient EMS versions

Upgrading from standard FortiClient EMS versions to FortiClient EMS for Chromebooks 1.2.2 is not supported.

Downgrading to previous versions

Downgrading FortiClient EMS for Chromebooks 1.2.2 to previous standard FortiClient EMS or FortiClient EMS for Chromebooks versions is not supported.

Resolved Issues

The following issues have been fixed in version 1.2.2.

Bug ID	Description
434328	ssl3 and tls1.0 cannot be disabled on EMS server
446697	Profile refuses to sync with 400+ web filter exclusions
448306	Scroll on load stops after the first 100 records

Known Issues

The following issues have been identified in version 1.2.2. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Bug ID	Description
454697	Add an option to find where profile is assigned



FORTINET®



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.